REMARKS/ARGUMENTS

I. Introduction:

Claims 1, 13, 18, 19, 22, 26, 29, and 30 are amended, claims 21 and 25 are canceled, and claims 37-44 are added herein. With entry of this amendment, claims 1-20, 22-24, and 26-44 will be pending.

II. Claim Rejections Under 35 U.S.C. 103:

Claims 1-18 and 36 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. in view of U.S. Patent No. 6,345,299 (Segal).

Vaid et al. disclose a directory enabled policy management tool for intelligent traffic management. The tool is used for monitoring or profiling quality of service within one or more information sources in a network of computers. The system includes applications or tools that are distributed over the network to monitor one or more nodes on the network. A bandwidth management tool is used to control incoming and outgoing traffic over the network. A flow analysis module implements traffic control based on a combination of flow control and queuing algorithms. QoS agents are distributed throughout the network to monitor and control bandwidth.

Claim 1 is directed to a method for propagating filters to an upstream device and generally includes: generating a filter at a first network device; sending information on the filter to a second network device located upstream from the first network device; and requesting the second network device to install a filter so that data is filtered closer to a source of the data. The method further includes sending routing information from the first network device to the second device so that the filter installed on the second network device filters traffic forwarded to the first network device without filtering traffic to other downstream nodes, and analyzing new data received at the first network

device and sending filter information to the second network device based on the analyzed data so that the second network device can refine the filter installed thereon. Claim 1 has been amended to clarify that the first network device installs a filter and that the data received and analyzed at the first network device is from the second network device.

Vaid et al. simply show agents distributed throughout a network. Vaid et al. do not disclose sending routing information from a first network device configured to filter traffic to a second network device so that a filter installed on the second network device filters traffic forwarded to the first network device without filtering traffic to other downstream nodes. Applicant's invention is particularly advantageous in that it shares filter information between a downstream node and an upstream node such that only traffic that would be forwarded to the requesting downstream node is affected. Importantly, this limits use of the system by an attacker as a means for carrying out a denial of service attack, for example. Furthermore, applicant's invention, as set forth in claim 1, analyzes new data received at the first network device and sends filter information to the second network device so that it can refine its filter, as needed. The distributed agents of Vaid et al. provide monitoring and control of incoming and outgoing traffic over a network. The agents are placed at a plurality of nodes (see Fig. 16) and coupled directly to a distributed policy management tool. There is no direct communication between downstream and upstream filtering nodes with information being exchanged between the two nodes to refine filters based on analysis of data at the associated node.

The Examiner asserts that Vaid et al. disclose exchanging filter information between a monitoring node and a server or administrator node. However, there is no exchange of filter information between two nodes configured specifically to filter data. Applicant's invention allows for the propagation of filter information from a filtering node directly to another filtering node to send filter data closer to the source of the data. Since the two filtering nodes can communicate directly with one another, filter

information can easily be exchanged in either direction between the two nodes. As noted by the Examiner, Vaid simply sends policy modifications from an administrative node out to a plurality of filtering nodes.

Furthermore, as noted by the Examiner, Vaid fails to teach filtering data closer to a source of data and sending routing information from a first network device to a second network device so that the filter installed on the second network device filters traffic forwarded to the first network device without filtering traffic to other downstream nodes.

Segal discloses a distributed security system for a communication network. The system includes a plurality of user nodes linked together within the network. Each user node includes means for transmitting information to other nodes in the network identifying allowed senders and receivers. The system further includes security nodes which detect transmission and relays each signal only to the recipients specified in the list. The security nodes simply pass lists containing access privileges for nodes between the security nodes. The nodes do not analyze incoming data in order to determine how to refine filters.

Neither Vaid et al. nor Segal show or suggest analyzing data received at a first network device having a filter installed thereon from a second network device also having a filter and sending information back to the second network device so that the second network device can refine its filter, as required by claim 1. This feature allows a downstream device to receive filter statistics from an upstream device. This is important because once the filter is installed on the upstream device, the downstream device will not see the traffic. If the downstream device determines that the filter is no longer required based on the analyzed flow, the device can send a message to the upstream device to remove or refine its filter.

Furthermore, Applicant respectfully submits that there is no suggestion to combine the teachings of Vaid et al. with Segal to produce the claimed invention.

Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. Vaid et al. use a monitoring/management tool (208 in Fig. 2) for traffic management and monitoring of quality of service. Whereas Segal simply transfers access control lists between security nodes, without interfacing with a central management tool. In fact, there is no monitoring of transmission. Segal even notes that using one centralized unit to handle communications for each network has significant limitations.

Accordingly, claim 1 is submitted as patentable over Vaid et al. and Segal. Claims 2-12, 22-24, 26, and 30-44, depending either directly or indirectly from claim 1, are submitted as patentable for the same reasons as claim 1.

Claim 36 is further submitted as patentable over Vaid et al. and Segal which do not show or suggest a filter propagation protocol utilized to exchange information between first and second network devices having filters installed thereon. In rejecting claim 36, the Examiner refers to col. 23, lines 40-42 of the Vaid et al. patent. This portion of the patent simply discusses translating policies into dynamic actions that are communicated to enforcement devices via a policy exchange protocol or standard network management protocol. In other words, policies are sent from management devices to network devices used to enforce the policies. Vaid et al. do not address the exchange of filter information directly between two network filtering devices.

Claims 13 and 18 have been amended to clarify that the data received and analyzed at the first network device is from the second network device, and are submitted as patentable for the same reasons discussed above with respect to claim 1. Claims 14-17, depending directly from claim 13, are submitted as patentable for the same reasons as claim 13.

Claims 19, 21-24, and 29 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. in view of U.S. Patent No. 6,141,686 (Jackowski et al.).

Claim 19 is directed to a method for installing filters on connected network devices and generally includes analyzing network flow received at a first network device, generating a filter at a second network device based on the analyzed flow, and propagating the filter from the second network device to the first network device. The method further includes generating filter statistics at the second network device, sending filter statistics to the first network device, and utilizing a filter propagation protocol to exchange information directly between the first and second network devices to refine the filter.

The system of Vaid et al. includes a meta-policy service which distributes policies to the agents which are used to monitor and control network traffic. There is no direct exchange of filter statistics between nodes which allow the filters to be refined according to the filter statistics generated at the associated node. As previously discussed, Vaid et al. do not show or suggest exchange of filter information between two nodes configured specifically to filter data or utilizing a filter propagation protocol to exchange information directly between the devices to refine the filter. As noted by the Examiner, Vaid et al. does not teach generating filtering statistics and sending statistics between a first and second network device.

Jackowski et al. disclose an application-classifier for intercepting network traffic and associating applications and users with network packets. These associations and statistics are consolidated into tables which a policy server can query to find which application is generating network traffic and prioritize the traffic based on the high-level application. A plugin is used to collect statistics on network traffic that can be read by a policy server.

The Jackowski et al. patent does not remedy the deficiencies of the Vaid et al. reference. Neither Vaid et al. nor Jackowski et al, either alone or in combination, show or suggest generating filter statistics at a filtering device and sending the filter statistics to another filtering device. Jackowski et al. are concerned with collecting statistics

relating to the use of high-level applications at a client or server machine and sending the information to a policy server.

Claim 19 is therefore submitted as patentable over Vaid et al. and Jackowski et al. Claims 20 and 29, depending directly from claim 19, are submitted as patentable for the same reasons as claim 19.

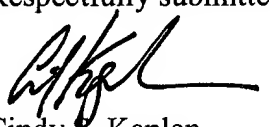
Claim 29 is further submitted as patentable over Vaid et al. and Jackowski et al. because they do not show or suggest reinstalling filters at predefined intervals to extend the lifetime of the filter and return packet and byte count statistics for the filter.

The additional references cited including U.S. Patent Nos. 5,883,901 (Chiu et al.), 6,098,172 (Coss et al.), and 6,665,725 (Dietz et al.), do not remedy the deficiencies of the primary references.

III. Conclusion:

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite prosecution of the application, please do not hesitate to call the undersigned at (408) 446-8695.

Respectfully submitted,



Cindy S. Kaplan
Reg. No. 40,043

RITTER, LANG & KAPLAN LLP
12930 Saratoga Ave., Suite D1
Saratoga, CA 95070
Tel: 408-446-8690
Fax: 408-446-8691